(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－196081

(43)公開日　平成11年(1999)７月21日

(51)Int.Cl.[6]		識別記号	FI		
H04L	9/08		H04L	9/00	601A
G09C	1/00	630	G09C	1/00	630E
H04L	9/14		H04L	9/00	601E
					641

審査請求　有　請求項の数4　FD　（全 16 頁）

(21)出願番号　特願平9－368942

(22)出願日　平成９年(1997)12月26日

(71)出願人　597174182
株式会社高度移動通信セキュリティ技術研究所
神奈川県横浜市港北区新横浜三丁目20番地８

(72)発明者　安齋　潤
神奈川県横浜市港北区新横浜三丁目20番地８　株式会社高度移動通信セキュリティ技術研究所内

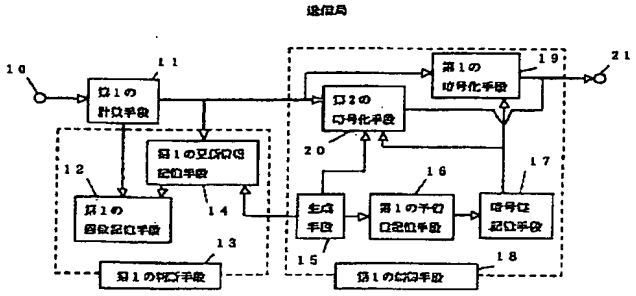
(74)代理人　弁理士　役　昌明　（外１名）

(54)【発明の名称】　暗号通信装置

(57)【要約】

【課題】　共通（秘密）鍵ブロック暗号を暗号通信と暗号鍵配送に用いる暗号通信装置において、安全かつ簡便に更新鍵を配送する。

【解決手段】　鍵更新の際、送信局において、予備鍵を新規暗号鍵とし、生成手段15で生成した予備鍵を新規予備鍵とし、予備鍵を暗号鍵で暗号化して送信し、その後、送信データを暗号鍵で暗号化して送信する。受信局においては、予備鍵を新規復号鍵とし、受信暗号化鍵を復号化して新規予備鍵とし、その後、受信暗号化データを復号化する。定期的に更新される予備の鍵を常に用意することにより、同じ鍵を暗号通信と鍵配送に一定の安全性で使用できる。鍵配送に使用する鍵は常に未使用なので安全性が高く、かつ配送用の鍵を管理（生成・更新）する手間を省くことができる。また、予備鍵や平文に応じて鍵更新のタイミングを決定することにより、予め送信局と受信局の間で鍵更新のタイミングを決定する必要が無く、かつ鍵更新のタイミングがランダムになるので、解読を容易にする情報が盗聴者に特定し難くなる。



【特許請求の範囲】

【請求項１】　送信局と受信局からなる暗号通信装置であって、前記送信局は、暗号鍵を記憶する暗号鍵記憶手段と、第１の予備鍵を記憶する第１の予備鍵記憶手段と、データを前記暗号鍵を用いて暗号化する第１の暗号化手段と、前記第１の予備鍵を前記暗号鍵を用いて暗号化する第２の暗号化手段と、前記第１の予備鍵を生成する生成手段と、前記第１の予備鍵を新規暗号鍵として前記暗号鍵記憶手段に転送し、前記生成手段により生成された予備鍵を新規第１の予備鍵として前記第１の予備鍵記憶手段に転送し、前記第２の暗号化手段の結果を出力し、その後前記第１の暗号化手段の結果を出力することを制御する第１の制御手段とを備え、前記受信局は、復号鍵を記憶する復号鍵記憶手段と、第２の予備鍵を記憶する第２の予備鍵記憶手段と、暗号化データを前記復号鍵を用いて復号化する第１の復号化手段と、前記第２の暗号化手段の結果を前記復号鍵を用いて復号化する第２の復号化手段と、前記第２の予備鍵を新規復号鍵として前記復号鍵記憶手段に転送し、前記第２の復号化手段の結果を新規第２の予備鍵として第２の予備鍵記憶手段に転送し、その後前記第１の復号化手段の結果を出力することを制御する第２の制御手段とを備えることを特徴とする暗号通信装置。

【請求項２】　送信局における前記第１の暗号化手段が、前記暗号鍵を用いて暗号化データを復号化し、受信局における前記第１の復号化手段が、前記復号鍵を用いてデータを暗号化することを特徴とする請求項１記載の暗号通信装置。

【請求項３】　前記受信局が、前記第２の暗号化手段の結果を記憶する暗号化予備鍵記憶手段と、前記第２の暗号化手段の結果を暗号化予備鍵記憶手段に転送し、前記第２の復号化手段の結果を新規復号鍵として前記復号鍵記憶手段に転送することを制御する第２の制御手段とを備えることを特徴とする請求項１記載の暗号通信装置。

【請求項４】　前記送信局は、送信回数を計数する第１の計数手段と、前記送信回数と前記送信回数上限値を記憶する第１の回数記憶手段と、更新情報を記憶する第１の更新情報記憶手段と、前記送信回数と前記送信回数上限値を調べ、前記送信回数上限値が一定値以下ならば前記送信回数上限値に一定値の加算を行ない、前記送信回数と前記送信回数上限値が等しいならば前記更新情報を前記送信回数上限値へ書き込み、更新開始の通知を行ない、その後新規更新情報の前記更新情報記憶手段への転送を行なう第１の判断手段とを備え、前記受信局は、受信回数を計数する第２の計数手段と、前記受信回数と前記受信回数上限値を記憶する第２の回数記憶手段と、前記受信回数と前記受信回数上限値を調べ、前記受信回数上限値が一定値以下ならば前記受信回数上限値に一定値の加算を行ない、前記受信回数と前記受信回数上限値が等しいならば前記更新情報を前記受信回数上限値へ書き込み、更新開始の通知を行ない、その後新規更新情報の前記更新情報記憶手段への転送を行なう第２の判断手段とを備えることを特徴とする請求項１記載の暗号通信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、送信局と受信局からなる暗号通信装置に関し、特に、共通（秘密）鍵ブロック暗号を暗号通信と暗号鍵配送に用いた暗号通信装置における鍵更新装置に関する。

【０００２】

【従来の技術】従来の共通（秘密）鍵ブロック暗号を、暗号通信と暗号鍵配送に用いた暗号通信装置は、鍵更新のための鍵配送方式として、更新用の新しい鍵を、鍵更新前まで使用していた鍵で暗号化して配送する（例えば、特開昭60-10834号公報）か、別に用意した配送用の鍵で暗号化して配送する（例えば、特開昭62-104238号公報）か、過去に使用された鍵で暗号化して配送する（例えば、特開平1-225251号公報）という手段を用いていた。

【０００３】また、鍵更新を行なうタイミングとして、暗号通信のたびや送信局か受信局から更新要求があったとき、または鍵の使用が一定時間に達したとき（例えば、特開昭62-181643号公報）等に鍵更新を行なっていた。

【０００４】図１１と図１２は、従来の暗号通信装置として、前記先行技術をいくつか組み合わせた例を示し、図１１は送信局の例、図１２は受信局の例を示す。点線で括られた範囲の各手段は判断手段または制御手段により制御される。

【０００５】従来の暗号通信装置では、鍵更新を行なうタイミングとして、（Ａ）暗号通信のたびに鍵更新を行なう方式や、（Ｂ）送信局か受信局から更新要求があったときに鍵更新を行なう方式や、（Ｃ）鍵の使用が一定時間に達したとき等に鍵更新を行なう方式があった。

（Ａ）と（Ｂ）の２方式が、図１１と図１２において、51、52、53、71、72、73が存在しない場合に対応し、（Ｃ）の方式が、図１１と図１２において、51、52、53、71、72、73が存在する場合に対応する。

【０００６】従来の（Ａ）方式暗号装置の場合、鍵の更新のタイミングを決定する手段は必要でない。

【０００７】（Ｂ）方式暗号装置の場合、鍵の更新のタイミングを決定する手段が存在しないので、送信局または受信局のユーザーは任意の手段を用いてタイミングを決定する必要がある。任意の手段としては、通信時間で更新するならばタイマー、送受信回数で更新するならばカウンター等が考えられる。

【０００８】（Ｃ）方式暗号装置の場合、従来の送信局では、第１の計数手段51で計数された送信回数が、第１の回数記憶手段52に記憶され、第１の判断手段53が前記

送信回数と第１の回数記憶手段52に記憶された送信回数上限値を比較して等しければ第１の制御手段60に更新開始を通知する。また、従来の受信局では、第２の計数手段71で計数された受信回数が、第２の回数記憶手段72に記憶され、第２の判断手段73が前記受信回数と第２の回数記憶手段72に記憶された受信回数上限値を比較して等しければ第２の制御手段77に更新開始を通知する。

【０００９】従来の暗号通信装置では、鍵更新のための鍵配送方式として、更新用の新しい鍵を、（Ｄ）鍵更新前まで使用していた鍵で暗号化して配送するか、（Ｅ）別に用意した配送用の鍵で暗号化して配送するか、過去に使用された鍵で暗号化して配送するという手段を用いていた。（Ｄ）が、図１１と図１２において、58、76の各手段が存在しない場合に対応し、（Ｅ）方式が、図１１と図１２において、58、76の各手段が存在する場合に対応する。

【００１０】（Ｄ）方式の場合、従来の送信局では、更新開始の通知を受けた第１の制御手段が以下の制御を行なう。第２の生成手段57で生成された新しい鍵を暗号鍵記憶手段55に記憶された既に暗号通信に使用してきた暗号鍵を用いて第２の暗号化手段59で暗号化して受信局に送信する。また、従来の受信局では、更新開始の通知を受けた第２の制御手段が以下の制御を行なう。受信した暗号化された新しい鍵を、復号鍵記憶手段75に記憶された既に暗号通信に使用してきた復号鍵を用いて第２の復号化手段76で復号化して新しい鍵を得る。

【００１１】（Ｅ）方式の場合、従来の送信局では、更新開始の通知を受けた第１の制御手段が以下の制御を行なう。第２の生成手段57で生成された新しい鍵を配送用暗号鍵記憶手段に記憶された配送用暗号鍵を用いて第２の暗号化手段59で暗号化して受信局に送信する。また、従来の受信局では、更新開始の通知を受けた第２の制御手段が以下の制御を行なう。受信した暗号化された新しい鍵を配送用復号鍵記憶手段76に記憶された配送用復号鍵を用いて第２の復号化手段76で復号化して新しい鍵を得る。

【００１２】

【発明が解決しようとする課題】上記従来の暗号通信装置においては、暗号通信に用いる鍵を更新するときに、更新用の新しい鍵を、鍵更新前まで使用していた鍵で暗号化して配送するか、過去に使用された鍵で暗号化して配送するという手段を用いていた。しかし、配送に用いる鍵が既に一定期間使用した鍵なので、鍵の安全性が低いという問題を有していた。

【００１３】また、別に用意した配送用の鍵で配送を行なう場合、暗号通信に使用する鍵とは別に、配送に使用する鍵を管理（生成・秘匿・更新）する必要が生じるという問題を有していた。

【００１４】暗号通信のたびに更新を行なう場合、常に暗号通信時間に更新処理時間が加わるために、実際に暗号通信が可能になるまでに時間がかかるという問題を有していた。

【００１５】また、鍵の使用が任意の時間に達したときの場合、タイミングの変更を行なうために送信局－受信局間で任意の時間を決定するためのやりとりが必要となるので、同じタイミングで更新を行なうことが多くなり、解読を容易にする情報（鍵を暗号化した暗号文がどれであるか、どこまでの暗号文が同じ鍵で暗号化されているか等）が盗聴者に知られる可能性が高くなるという問題を有していた。

【００１６】また、送信局または受信局から更新要求があったときの場合、ユーザーに更新判断が依存するためユーザーに負担となり、かつ更新判断の信頼性も低いという問題を有していた。

【００１７】本発明は、上記従来の問題を解決するもので、定期的に更新される予備の鍵を常に用意することにより、使用時期をずらして、同じ鍵を暗号通信と配送に一定の安全性で使用できるようにしたものである。配送に使用する鍵は常に未使用なので安全性が高く、かつ配送用の鍵を管理（生成・更新）する手間を省くことができる優れた暗号通信装置を提供することを第１の目的とする。

【００１８】また、受信局の配送鍵を暗号化しておくことにより、管理（秘匿）する手間を省くことができる優れた暗号通信装置を提供することを第２の目的とする。

【００１９】また、予備鍵や平文に依存して更新のタイミングを決定することにより、更新のタイミングを変更するたびに送信局－受信局間でやりとりする必要が無く、かつ更新のタイミングがランダムになるので、上記の解読を容易にする情報が盗聴者に特定し難くなる優れた暗号通信装置を提供することを第３の目的とする。

【００２０】

【課題を解決するための手段】本発明では、上記課題を解決するために、暗号通信装置の送信局においては、予備鍵を新規暗号鍵とし、生成手段により生成された予備鍵を新規予備鍵とし、予備鍵を暗号鍵で暗号化して送信し、その後、送信データを暗号鍵で暗号化して送信する構成とし、受信局においては、予備鍵を新規復号鍵とし、受信暗号化鍵を復号化して予備鍵とし、その後、受信暗号化データを復号化する構成とした。このように構成したことにより、予備の鍵を用意して常に未使用の鍵で新しい鍵を配送するので安全性が高くなり、同じ鍵を暗号通信と鍵配送に使用しても安全かつ簡便に暗号通信に使用する鍵を更新でき、かつ配送用の鍵を管理（生成・更新）する手間を省くことができる。

【００２１】また、暗号通信装置の受信局において、受信暗号化鍵を暗号化予備鍵として記憶し、鍵更新の際に、暗号化予備鍵を復号化して新規復号鍵とする構成とした。このように構成したことにより、受信局において予備鍵を管理（秘匿）する手間を省くことができる。

【００２２】また、暗号通信装置の送信局の判断手段で、送信回数と送信回数上限値を調べ、送信回数上限値が一定値以下ならば送信回数上限値に一定値の加算を行ない、送信回数と送信回数上限値が等しいならば更新情報を送信回数上限値へ書き込み、更新開始の通知を行ない、その後、新しい更新情報の更新情報記憶手段への転送を行なう構成とし、受信局の判断手段で、受信回数と受信回数上限値を調べ、受信回数上限値が一定値以下ならば受信回数上限値に一定値の加算を行ない、受信回数と受信回数上限値が等しいならば更新情報を受信回数上限値へ書き込み、更新開始の通知を行ない、その後、新しい更新情報の更新情報記憶手段への転送を行なう構成とした。このように構成したことにより、予備鍵や平文に依存して更新のタイミングを決定して、更新のタイミングを変更するたびに送信局－受信局間でやりとりする必要を無くし、かつ更新のタイミングがランダムになり、解読を容易にする情報を盗聴者が特定し難くなる。

【００２３】

【発明の実施の形態】本発明の請求項１に記載の発明は、送信局と受信局からなる暗号通信装置であって、前記送信局は、暗号鍵を記憶する暗号鍵記憶手段と、第１の予備鍵を記憶する第１の予備鍵記憶手段と、データを前記暗号鍵を用いて暗号化する第１の暗号化手段と、前記第１の予備鍵を前記暗号鍵を用いて暗号化する第２の暗号化手段と、前記第１の予備鍵を生成する生成手段と、前記第１の予備鍵を新規暗号鍵として前記暗号鍵記憶手段に転送し、前記生成手段により生成された予備鍵を新規第１の予備鍵として前記第１の予備鍵記憶手段に転送し、前記第２の暗号化手段の結果を出力し、その後前記第１の暗号化手段の結果を出力することを制御する第１の制御手段とを備え、前記受信局は、復号鍵を記憶する復号鍵記憶手段と、第２の予備鍵を記憶する第２の予備鍵記憶手段と、暗号化データを前記復号鍵を用いて復号化する第１の復号化手段と、前記第２の暗号化手段の結果を前記復号鍵を用いて復号化する第２の復号化手段と、前記第２の予備鍵を新規復号鍵として前記復号鍵記憶手段に転送し、前記第２の復号化手段の結果を新規第２の予備鍵として第２の予備鍵記憶手段に転送し、その後前記第１の復号化手段の結果を出力することを制御する第２の制御手段とを備える暗号通信装置であり、定期的に更新される予備の鍵を常に用意し、使用時期をずらして、同じ鍵を暗号通信と配送に一定の安全性で使用できるようにするという作用を有する。

【００２４】本発明の請求項２に記載の発明は、請求項１記載の暗号通信装置において、送信局における前記第１の暗号化手段が、前記暗号鍵を用いて暗号化データを復号化し、受信局における前記第１の復号化手段が、前記復号鍵を用いてデータを暗号化するものであり、受信局から送信局に暗号化データを送ることを可能にするという作用を有する。

【００２５】本発明の請求項３に記載の発明は、請求項１記載の暗号通信装置において、前記受信局が、復号鍵を記憶する復号鍵記憶手段と、前記第２の暗号化手段の結果を記憶する暗号化予備鍵記憶手段と、前記第１の暗号化手段の結果を前記復号鍵を用いて復号化する第１の復号化手段と、前記第２の暗号化手段の結果を前記復号鍵を用いて復号化する第２の復号化手段と、前記第２の暗号化手段の結果を暗号化予備鍵記憶手段に転送し、前記第２の復号化手段の結果を新規復号鍵として前記復号鍵記憶手段に転送することを制御する第２の制御手段とを備えるものであり、受信局の配送鍵を暗号化しておくことにより、管理（秘匿）する手間を省くという作用を有する。

【００２６】本発明の請求項４に記載の発明は、請求項１記載の暗号通信装置において、前記送信局は、送信回数を計数する第１の計数手段と、前記送信回数と前記送信回数上限値を記憶する第１の回数記憶手段と、更新情報を記憶する第１の更新情報記憶手段と、前記送信回数と前記送信回数上限値を調べ、前記送信回数上限値が一定値以下ならば前記送信回数上限値に一定値の加算を行ない、前記送信回数と前記送信回数上限値が等しいならば前記更新情報を前記送信回数上限値へ書き込み、更新開始の通知を行ない、その後新規更新情報の前記更新情報記憶手段への転送を行なう第１の判断手段とを備え、前記受信局は、受信回数を計数する第２の計数手段と、前記受信回数と前記受信回数上限値を記憶する第２の回数記憶手段と、前記受信回数と前記受信回数上限値を調べ、前記受信回数上限値が一定値以下ならば前記受信回数上限値に一定値の加算を行ない、前記受信回数と前記受信回数上限値が等しいならば前記更新情報を前記受信回数上限値へ書き込み、更新開始の通知を行ない、その後新規更新情報の前記更新情報記憶手段への転送を行なう第２の判断手段とを備えるものであり、予備鍵や平文に応じて更新のタイミングを決定し、解読を容易にする情報を特定し難くするという作用を有する。

【００２７】以下、本発明の実施の形態について、図１から図１０を用いて詳細に説明する。

【００２８】(第１の実施の形態) 本発明の第１の実施の形態は、送信局において、予備鍵を暗号鍵で暗号化した結果を送信し、その後データを暗号鍵で暗号化した結果を送信し、受信局において、予備鍵記憶手段にある予備鍵を新規復号鍵として復号鍵記憶手段に転送し、受信暗号化予備鍵を復号鍵で復号した結果を予備鍵記憶手段に出力し、その後、受信暗号化データを復号鍵で復号した結果を出力する暗号通信装置である。

【００２９】図１は、本発明の第１の実施の形態の暗号通信装置の送信局のブロック図である。図１において、点線で括られた範囲の各手段は、判断手段または制御手段により制御される。

【００３０】図１において、入力端子10は、送信時に平

文データの入力を行なうものであり、コネクターで構成されている。

【００３１】第１の計数手段11は、データの送信回数を計数するものであり、実際には、データの送信が行なわれるごとに、第１の回数記憶手段12に記憶された送信回数に１を加算するもので、ＲＯＭやＲＡＭを内蔵したマイクロプロセッサ、例えばＣＰＵやＤＳＰ等に計数アルゴリズムをプログラムした計数専用ＬＳＩとしたもので構成される。

【００３２】第１の回数記憶手段12は、第１の計数手段11で計数された現在の送信回数と、鍵更新のタイミングを決定する送信回数上限値を記憶するメモリであり、例えばＲＡＭ等で構成される。

【００３３】第１の判断手段13は、第１の回数記憶手段12に記憶されたデータの送信回数が一定の回数以上に達したか判定するとともに、送信回数上限値を更新するものであり、実際には、第１の回数記憶手段12に記憶されている現在の送信回数と送信回数上限値を比較し、等しければ第１の更新情報記憶手段14に記憶されている更新情報を第１の回数記憶手段12に転送し、第１の制御手段18に更新開始を通知し、新規更新情報を第１の更新情報記憶手段14に転送する操作と、第１の回数記憶手段12の送信回数上限値が予め設定した数以下ならば一定値を加算する操作を行なうもので、ＲＯＭやＲＡＭを内蔵したマイクロプロセッサ、例えばＣＰＵ、ＤＳＰ等に判断アルゴリズムをプログラムした判断専用ＬＳＩとしたもので構成される。送信回数上限値の更新は、第１の更新情報記憶手段14から転送されてくる更新情報を、第１の回数記憶手段12の送信回数上限値に上書きすることで行なう。ただし、送信回数上限値が０回では更新ばかり行なわれ、暗号通信状態に移行しないという問題が生じる。また、頻繁に一桁の回数で更新が行なわれると処理時間が増加して運用に支障をきたす。この問題を回避するために、送信回数上限値が０回や一桁の回数のときには、一定値を加算する操作を行なう。また、送信回数上限値の有効範囲と加算値は、実際の通信頻度により決定するべきである。更新情報としては予備鍵や平文を用いることが考えられる。予備鍵の場合には、第１の生成手段15で生成された予備鍵の特定の位置（例えば先頭または後尾）から一定数のビットを、第１の更新情報記憶手段14に転送する。平文の場合には、鍵更新後に最初に暗号化して送信する平文の特定の位置（例えば先頭または後尾）から一定数のビットを更新情報記憶手段に転送する。また、転送する更新情報を何ビットにするかで、鍵更新の期間を一定範囲に決定することができ、例えば８ビットにすれば０～255回の範囲に決定することができる。

【００３４】第１の更新情報記憶手段14は、更新情報を記憶するメモリであり、例えばＲＡＭ等で構成される。

【００３５】生成手段15は、予備鍵（疑似乱数）を生成するものであり、ＲＯＭやＲＡＭを内蔵したマイクロプロセッサ、例えばＣＰＵ・ＤＳＰ等に生成アルゴリズムをプログラムした生成専用ＬＳＩとしたもので構成される。乱数生成アルゴリズムとしては、ＬＦＳＲ(Liner Feedback Shift Registers)を用いるのが一般的である。しかし、兼用が可能であれば暗号アルゴリズムやハッシュアルゴリズムを用いることもある。また、疑似乱数生成にはシードと呼ばれる初期値が必要であり、例えばＣＰＵ・ＤＳＰ等のシステムクロックをシードとして利用することができる。

【００３６】第１の予備鍵記憶手段16は、第１の生成手段15で生成された予備鍵を記憶するメモリであり、例えばＲＡＭ等で構成される。

【００３７】暗号鍵記憶手段17は、第１の暗号化手段19と第２の暗号化手段20で暗号化に用いる暗号鍵を記憶するメモリであり、例えばＲＡＭ等で構成される。

【００３８】第１の制御手段18は、更新開始の通知を受けると、以下の動作を順番に行なうように制御するものであり、ＲＯＭやＲＡＭを内蔵したマイクロプロセッサ、例えばＣＰＵ・ＤＳＰ等に制御アルゴリズムをプログラムした制御専用ＬＳＩとしたもので構成される。初めに、第１の予備鍵記憶手段16に予め記憶されている予備鍵を暗号鍵記憶手段17に転送し、次に生成手段15に予備鍵の生成を指示し、次にこの生成された予備鍵を新規予備鍵として第１予備鍵記憶手段16と第２の暗号化手段20に転送し、次にこの予備鍵の暗号化を第２の暗号化手段20に指示し、最後にこの暗号化暗号鍵を受信局に送信する。

【００３９】第１の暗号化手段19は、暗号鍵記憶手段17に記憶されている暗号鍵を用いてデータを暗号化するものであり、ＲＯＭやＲＡＭを内蔵したマイクロプロセッサ、例えばＣＰＵ・ＤＳＰ等に暗号アルゴリズムをプログラムした暗号専用ＬＳＩとしたもので構成される。しかし、ＲＯＭやＲＡＭを内蔵したマイクロプロセッサ、例えばＣＰＵ・ＤＳＰ等に暗号アルゴリズムをプログラムするのが面倒であれば、初めから暗号専用のＬＳＩとして開発され市販されているものを使用することもできる。また、本発明では暗号として共通（秘密）鍵ブロック暗号を用いており、その種類としてＤＥＳ・ＦＥＡＬ・ＩＤＥＡ等が挙げられるが、どの暗号を用いても本発明は有効であると考えられる。

【００４０】第２の暗号化手段20は、暗号鍵記憶手段17に記憶されている暗号鍵を用いて鍵を暗号化するものであり、第１の暗号化手段と同じものである。

【００４１】出力端子21は、送信時には暗号化データの出力を行ない、受信時には平文データの出力を行なうものであり、コネクター等で構成されている。

【００４２】図２は、本発明の第１の実施の形態の暗号通信装置の受信局のブロック図である。図２において、点線で括られた範囲の各手段は、判断手段または制御手

段により制御される。図２において、入力端子30は、受信時に暗号化データの入力を行なうものであり、コネクターで構成されている。

【００４３】第２の計数手段31は、データの受信回数を計数するものであり、実際にはデータの受信が行なわれるごとに、第２の回数記憶手段32に記憶された受信回数に１を加算するもので、ＲＯＭやＲＡＭを内蔵したマイクロプロセッサ、例えばＣＰＵやＤＳＰ等に計数アルゴリズムをプログラムした計数専用ＬＳＩとしたもので構成される。

【００４４】第２の回数記憶手段32は、第２の計数手段31で計数された現在の受信回数と鍵更新のタイミシグを決定する受信回数上限値を記憶するメモリであり、例えばＲＡＭ等で構成される。

【００４５】第２の判断手段33は、第２の回数記憶手段32に記憶されたデータの受信回数が一定の回数以上に達したか判定するとともに、受信回数上限値を更新するものであり、実際には、回数記憶手段32に記憶されている現在の受信回数と、予め設定されている受信回数上限値を比較し、等しければ第２の更新情報記憶手段34に記憶されている更新情報を第２の回数記憶手段32に転送し、第２の制御手段37に更新開始を通知し、新規更新情報を更新情報記憶手段34に転送する操作と、第２の回数記憶手段32の受信回数上限値が予め設定した数以下ならば一定値を加算する操作を行なうもので、ＲＯＭやＲＡＭを内蔵したマイクロプロセッサ、例えばＣＰＵ・ＤＳＰ等に判断アルゴリズムをプログラムした判断専用ＬＳＩとしたもので構成される。受信回数上限値の更新は、第２の更新情報記憶手段34から転送されてくる更新情報を第２の回数記憶手段32の受信回数上限値に上書きすることで行なう。ただし、受信回数上限値が０回では更新ばかり行なわれ暗号通信状態に移行しないという問題が生じる。また、頻繁に一桁の回数で更新が行なわれると処理時間が増加して運用に支障をきたす。この問題を回避するために、受信回数上限値が０回や一桁の回数のときには一定値を加算する操作を行なう。また、受信回数上限値の有効範囲と加算値は、実際の通信頻度により決定するべきである。更新情報としては予備鍵や平文を用いることが考えられる。予備鍵を用いるには、第２の復号化手段38で復号化された予備鍵の特定の位置（例えば先頭または後尾）から一定数のビットを第２の更新情報記憶手段に転送する。平文の場合には、鍵更新後に最初に受信して第１の復号化手段39で復号化した平文の特定の位置（例えば先頭または後尾）から一定数のビットを第２の更新情報記憶手段34に転送する。また、転送する更新情報を何ビットにするかで鍵更新の期間を一定範囲に決定することができ、例えば８ビットにすれば０～255回の範囲に決定できる。

【００４６】第２の更新情報記憶手段34は、更新情報を記憶するメモリであり、例えばＲＡＭ等で構成される。

【００４７】第２の予備鍵記憶手段35は、予備鍵を記憶するメモリであり、例えばＲＡＭ等で構成される。

【００４８】復号鍵記憶手段36は、復号鍵を記憶するメモリであり、例えばＲＡＭ等で構成される。

【００４９】第２の制御手段37は、更新開始の通知を受けると、以下の動作を順番に行なうように制御するものであり、ＲＯＭやＲＡＭを内蔵したマイクロプロセッサ、例えばＣＰＵ・ＤＳＰ等に制御アルゴリズムをプログラムした制御専用ＬＳＩとしたもので構成される。初めに、第２の予備鍵記憶手段35に予め記憶されている予備鍵を新規復号鍵として復号鍵記憶手段36に転送し、次に受信した暗号化予備鍵を第２の復号化手段38に転送し、次に第２の復号化手段38に前記暗号化予備鍵の復号化を指示し、最後に復号化された予備鍵を新規予備鍵として第２の予備鍵記憶羊段に転送する。

【００５０】第１の復号化手段38は、復号鍵記憶手段36に記憶された復号鍵を用いてデータを復号化するものであり、ＲＯＭやＲＡＭを内蔵したマイクロプロセッサ、例えばＣＰＵ・ＤＳＰ等に暗号アルゴリズムをプログラムした暗号専用ＬＳＩとしたもので構成される。しかし、ＲＯＭやＲＡＭを内蔵したマイクロプロセッサ、例えばＣＰＵ・ＤＳＰ等に暗号アルゴリズムをプログラムするのが面倒であれば、送信局と同様に初めから暗号専用のＬＳＩとして開発されたものを使用することもできる。また、本発明では暗号として共通（秘密）鍵ブロック暗号を用いており、その種類としてＤＥＳ・ＦＥＡＬ・ＩＤＥＡ等が挙げられるが、どの暗号を用いても本発明は有効であると考えられる。

【００５１】第２の復号化手段39は、復号鍵記憶手段36に記憶された復号鍵を用いて鍵を復号化するものであり、第１の復号化手段と同じものである。

【００５２】出力端子40は、受信時にデータの出力を行なうものであり、コネクターで構成されている。

【００５３】以上のように構成された暗号通信装置について、図３と図４を用いて、その動作を説明する。ここで図３が送信局の動作、図４が端末機の動作を示す。図３について説明する。

【００５４】初めに、入力として受信局へ送信する通信文（平文）を考える。ステップ１～４までが鍵更新プロセスへの移行を判断するプロセスである。

【００５５】ステップ１・２では、第１の計数手段11が入力として送信データが送られて来たことを確認し、第１の回数記憶手段12に記憶されている送信回数に１を加算する。

【００５６】ステップ３では、第１の回数記憶手段12に記憶されている送信回数上限値がＬ以下であれば上限値に一定値を加算する。

【００５７】ステップ４では、第１の回数記憶手段12に記憶されている送信回数と送信回数の上限Ｍを比較し、等しければ第１の制御手段13に更新開始を通知し、そう

でなければステップ１に戻る。ステップ５以降の動作は全て第１の制御手段13により順番に実行される鍵更新プロセスである。

【００５８】ステップ５では、第１の更新情報記憶手段14に記憶されている更新情報を第１の回数記憶手段12の送信回数上限値に上書きする。

【００５９】ステップ６では、第１の予備鍵記憶手段16に記憶されている予備鍵を新規暗号鍵として暗号鍵記憶手段17に転送する。

【００６０】ステップ７では、生成手段15で予備鍵(疑似乱数)を生成する。

【００６１】ステップ８では、ステップ７で生成された予備鍵を新規予備鍵として第１の予備鍵記憶手段16と第２の暗号化手段20に転送する。

【００６２】ステップ９では、ステップ８で第２の暗号化手段20に転送された予備鍵を暗号鍵記憶手段17に記憶されている暗号鍵で暗号化する。

【００６３】ステップ10では、ステップ９で生成された暗号化予備鍵を受信局に送信する. ステップ11では、新規更新情報を第１の更新情報記憶手段14に転送する。ステップ11終了後、出力として更新された暗号鍵を用いて通信文（入力平文）を暗号化して出力する。

【００６４】図４について説明する。ステップ１～４までが鍵更新プロセスへの移行を判断するプロセスである。

【００６５】ステップ１・２では、第２の計数手段31が入力として受信データが送られて来たことを確認し、第２の回数記憶手段32に記憶されている受信回数に１を加算する。

【００６６】ステップ３では、第２の判断手段33が第２の回数記憶手段32に記憶されている受信回数上限値がL以下であれば上限値に一定値を加算する。

【００６７】ステップ４では、第２の回数記憶手段32に記憶されている受信回数上限値が第２の回数記憶手段32に記憶されている受信回数と受信回数の上限Mを比較し、等しければ第２の制御手段33に更新開始を通知し、そうでなければステップ１に戻る。ステップ５以降の動作は全て第２の制御手段37により順番に実行される鍵更新プロセスである。

【００６８】ステップ５では、第２の更新情報記憶手段34に記憶されている更新情報を第２の回数記憶手段32の受信回数上限値に書き込む。

【００６９】ステップ６では、第２の予備鍵記憶手段35に記憶された予備鍵を復号鍵記憶手段36に転送する。

【００７０】ステップ７では、受信した暗号化予備鍵を第２の復号化手段39に転送する。

【００７１】ステップ８では、ステップ７で転送した暗号化予備鍵を第２の復号化手段39で復号鍵記憶手段36に記憶された復号鍵を用いて復号化する。

【００７２】ステップ９では、ステップ８で復号化された予備鍵を新規復号鍵として第２の予備鍵記憶手段35に転送する。

【００７３】ステップXは、新規更新情報が平文か予備鍵かで実行されるタイミングが異なる。予備鍵であれば、予備鍵が復号化されるステップ８終了後に実行される。平文の場合には、鍵更新終了後に最初に受信した暗号文を復号化して得られる平文を入手した後に実行される。

【００７４】図５は、送信局と受信局を接続した暗号通信装置全体の構成について示したものである。本発明では、送信局の入出力端子21と受信局の入出力端子30の接続は有線を想定しており、ケーブル、例えば同軸ケーブルで構成される。また、本発明の鍵更新装置は無線通信システムにも使用可能であると考えられる。図５では、説明の簡単化のために受信局は１台しか示していないが、実際には複数の受信局を想定している。これは送信局が基地局で、受信局が端末局のような場合も考えているからである。受信局が複数の場合にも受信局側はこれまでの説明と同様である。しかし、送信局は受信局の台数だけ鍵更新を行なう必要があるので、鍵と送信回数と送信回数上限値を受信局ごとに分けて記憶しなければならない。つまり、送信局の第１の回数記憶手段と第１の予備鍵記憶手段と第１の暗号鍵記憶手段にはそれぞれ受信局ごとの送信回数と送信回数上限値と予備鍵と暗号鍵を記憶しておく。

【００７５】実装上の留意点としては、送信局の第１の計数手段11、第１の判断手段13、第１の制御手段18、生成手段15、第１の暗号化手段19、第２の暗号化手段20を個々にマイクロプロセッサーを用いて構成すると効率が悪いので、性能に問題がなければ一つのマイクロプロセッサーで兼用するのが望ましい。また、受信局についても同様に第２の計数手段31、第２の判断手段33、第２の制御手段37、第１の復号化手段38、第２の復号化手段39を一つのマイクロプロセッサーで兼用するのが望ましい。

【００７６】図６と図７は、各通信状態における鍵の配置を示したもので、横方向が通信状態、縦方向が鍵の状態を表す。

【００７７】図６に示す送信局の場合は以下のように鍵の状態が推移する。

【００７８】状態:１は、通信を行なう前の準備段階であり、初めに鍵Ａと鍵Ｂをセットする。また、このとき同時に鍵を更新する送信回数および受信回数の上限値の初期値を送信局と受信局の間で決定しておく。

【００７９】状態:２は、最初の暗号通信状態であり、暗号鍵記憶手段の暗号鍵Ａで暗号通信を行ない、第１の予備鍵記憶手段16の予備鍵Ｂは使用しない。送信回数が一定値に達した時点で状態:３へ移行する。

【００８０】状態:３は、最初の鍵更新状態であり、第１の予備鍵記憶手段16の予備鍵Ｂを新規暗号鍵として暗

号鍵記憶手段17に転送して暗号鍵Ｂとする。これにより暗号鍵Ａは廃棄されたことになる。次に鍵Ｃを生成し、第１の予備鍵記憶手段16に新規予備鍵として転送する。最後に予備鍵Ｃを暗号鍵Ｂで暗号化して送信し、状態:４に移行する。

【００８１】状態:４は、暗号通信状態であり、暗号鍵記憶手段17の暗号鍵Ｂで暗号通信を行ない、第１の予備鍵記憶手段16の予備鍵Ｃは使用しない。送信回数上限値が一定値に達した時点で状態:５へ移行する。

【００８２】状態:５は鍵更新状態であり、第１の予備鍵記憶手段16の予備鍵Ｃを新規暗号鍵として暗号鍵記憶手段17に転送して暗号鍵Ｃとする。これにより暗号鍵Ｂは廃棄されたことになる。次に鍵Ｄを生成し、第１の予備鍵記憶手段16に新規予備鍵として転送する。最後に予備鍵Ｄを暗号鍵Ｃで暗号化して送信し、状態:６に移行する。

【００８３】状態:６は、暗号通信状態であり、暗号鍵記憶手段17の暗号鍵Ｃで暗号通信を行ない、第１の予備鍵記憶手段16の予備鍵Ｄは使用しない。以下、鍵配送状態と暗号通信状態が交互に繰り返される。

【００８４】図７に示す受信局の場合は、以下のように鍵の状態が推移する。

【００８５】状態:１は、通信を行なう前の準備段階であり、初めに鍵Ａと鍵Ｂをセットしておく。また、このとき同時に鍵を更新する送信回数および受信回数の上限値の初期値を送信局と受信局の間で決定しておく。

【００８６】状態:２は、最初の暗号通信状態であり、復号鍵記憶手段36の復号鍵Ａで暗号通信を行ない、第２の予備鍵記憶手段35の予備鍵Ｂは使用せず、受信回数が一定値に達した時点で状態:３へ移行する。

【００８７】状態:３は、最初の鍵更新状態であり、第２の予備鍵記憶手段35の予備鍵Ｂを新規復号鍵として復号鍵記憶手段36に転送して復号鍵Ｂとする。よって、復号鍵Ａは廃棄されたことになる。次に暗号化Ｃを受信し、復号鍵Ｂで復号化して新規予備鍵として第２の予備鍵記憶装置35に転送する。鍵更新終了後、状態:４に移行する。

【００８８】状態:４は、暗号通信状態であり、復号鍵記憶手段36の復号鍵Ｂで暗号通信を行ない、第２の予備鍵記憶手段35の予備鍵Ｃは使用しない。受信回数が一定値に達した時点で、状態:５へ移行する。

【００８９】状態:５は、鍵更新状態であり、第２の予備鍵記憶手段35の予備鍵Ｃを新規復号鍵として復号鍵記憶手段36に転送して復号鍵Ｃとする。よって、復号鍵Ｂは廃棄されたことになる。次に暗号化Ｄを受信し、復号鍵Ｃで復号化して新規予備鍵として第２の予備鍵記憶装置35に転送する。鍵更新終了後、状態:６に移行する。

【００９０】状態:６は、暗号通信状態であり、復号鍵記憶手段36の復号鍵Ｃで暗号通信を行ない、第２の予備鍵記憶手段35の予備鍵Ｄは使用しない。以下、鍵配送状態と暗号通信状態が交互に繰り返される。

【００９１】最後に、従来の暗号通信装置と本発明の鍵の更新による安全性が全体としてみたときにはどのように考えられるかを説明する。本発明では、使用時間をずらすことにより暗号用の鍵と配送用の鍵を一つの鍵で共有している。この方法は配送用の鍵に暗号通信に未使用の鍵を用いているので、配送用の鍵を用意しない場合よりは安全性が高い。ただし、盗聴者が暗号用の鍵を解読でき、かつ以前に配送された予備鍵を暗号化した暗号文を保持していると、別に配送用の鍵を用意する場合より安全性が低くなる場合がある。しかし、鍵の更新のタイミングをランダムにすることにより、予備鍵を暗号化した暗号文を特定し難くしてある。したがって、別に配送用の鍵を用意する場合において同じ配送鍵を使い続ければ、本発明の安全性の方が高くなっていく可能性が高い。

【００９２】上記のように、本発明の第１の実施の形態では、暗号通信装置を、送信局において、予備鍵を暗号鍵で暗号化した結果を送信し、その後データを暗号鍵で暗号化した結果を送信し、受信局において、予備鍵記憶手段にある予備鍵を新規復号鍵として復号鍵記憶手段に転送し、受信暗号化予備鍵を復号鍵で復号した結果を予備鍵記憶手段に出力し、その後、受信暗号化データを復号鍵で復号した結果を出力する構成としたので、未使用の鍵で予備鍵を配送するので、鍵配送の安全性が高くなる。

【００９３】(第２の実施の形態) 本発明の第２の実施の形態は、受信局において、受信暗号化予備鍵を暗号化予備鍵記憶手段に転送し、鍵更新の際に、暗号化予備鍵記憶手段の暗号化予備鍵を復号鍵で復号した結果を新規復号鍵として復号鍵記憶手段に転送する暗号通信装置である。

【００９４】第２の実施の形態の暗号通信装置が、第１の実施の形態と異なるところは、予備鍵を受信側で暗号化予備鍵のままで記憶しておき、復号鍵として使用する直前に複号する点である。

【００９５】図８は、本発明の第２の実施の形態の暗号通信装置の受信局のブロック図である。図８において、入力端子30、第２の計数手段31、第２の回数記憶手段32、第２の判断手段33、第２の更新情報記憶手段34、復号鍵記憶手段36、第１の復号化手段38、第２の復号化手段39、出力端子40は、第１の実施の形態と同じである。

【００９６】暗号化予備鍵記憶手段35は、受信した暗号化予備鍵を記憶するメモリである。

【００９７】第２の制御手段37は、更新開始の通知を受けると、以下の動作を順番に行なうように制御するものである。初めに、暗号化予備鍵記憶手段35の暗号化予備鍵を第２の復号化手段38に転送し、次に前記暗号化予備鍵の復号化を第２の復号化手段38に指示し、次に復号化された予備鍵を新規復号鍵として復号鍵記憶手段36に転

送し、最後に受信した暗号化予備鍵を新規暗号化予備鍵として暗号化予備鍵記憶手段に転送する。

【００９８】以上のように構成された暗号通信装置について、図９に示す受信局のフローチャートを用いて受信局の動作を説明する。送信局の動作は第１の実施の形態と同じである。ステップ１～５までのプロセスは、第１の実施の形態と同じである。

【００９９】ステップ６では、暗号化予備鍵記憶手段35'に記憶されている暗号化予備鍵を第２の復号化手段39に転送する。

【０１００】ステップ７では、ステップ６で転送した暗号化予備鍵を第２の復号化手段39で復号鍵記憶手段36に記憶された復号鍵を用いて復号する。

【０１０１】ステップ８では、ステップ７で復号化された予備鍵を新規復号鍵として復号鍵記憶手段36に転送する。

【０１０２】ステップ９では、受信した暗号化予備鍵を新規暗号化予備鍵として暗号化予備鍵記憶手段35'に転送する。

【０１０３】ステップXは、新規更新情報が平文か予備鍵かで実行されるタイミングが異なる。予備鍵であれば、予備鍵が復号化されるステップ８終了後に実行される。平文の場合には、鍵更新終了後に最初に受信した暗号文を復号化して得られる平文を入手した後に実行される。

【０１０４】図１０は、受信局の各通信状態における鍵の配置を示したもので、横方向が通信状態、縦方向が鍵の状態を表す。以下のように鍵の状態が推移する。

【０１０５】状態:１は、通信を行なう前の準備段階であり、初めに鍵Ａと、鍵Ｂを鍵Ａで暗号化した暗号化Ｂをセットしておく。また、このとき同時に鍵を更新する送信回数および受信回数の上限値の初期値を送信局と受信局の間で決定しておく。

【０１０６】状態:２は、最初の暗号通信状態であり、復号鍵記憶手段36の復号鍵Ａで暗号通信を行ない、暗号化予備鍵記憶手段35'の暗号化Ｂは使用しない。受信回数が一定値に達した時点で状態:３へ移行する。

【０１０７】状態:３は、最初の鍵更新状態であり、暗号化予備鍵記憶手段35'の暗号化Ｂを復号鍵Ａで復号化して復号鍵記憶手段36に転送する。よって、復号鍵Ａは廃棄されたことになる。次に暗号化Ｃを受信し、暗号化予備鍵記憶手段35'に新規暗号化予備鍵として転送する。鍵更新終了後、状態:４に移行する。

【０１０８】状態:４は、暗号通信状態であり、復号鍵記憶手段36の復号鍵Ｂで暗号通信を行ない、暗号化予備鍵記憶手段35'の暗号化Ｃは使用しない。受信回数が一定値に達した時点で状態:５へ移行する。

【０１０９】状態:５は、鍵更新状態であり、暗号化予備鍵記憶手段35'の暗号化Ｃを復号鍵Ｂで復号化して復号鍵記憶手段36に転送する。よって、復号鍵Ｂは廃棄されたことになる。次に暗号化Ｄを受信し、暗号化予備鍵記憶手段35'に新規暗号化予備鍵として転送する。鍵更新終了後、状態:６に移行する。

【０１１０】状態:６は、暗号通信状態であり、復号鍵記憶手段36の復号鍵Ｃで暗号通信を行ない、暗号化予備鍵記憶手段35'の暗号化Ｄは使用しない。以下、鍵配送状態と暗号通信状態が交互に繰り返される。

【０１１１】上記のように、本発明の第２の実施の形態では、暗号通信装置を、受信局において、受信暗号化予備鍵を暗号化予備鍵記憶手段に転送し、鍵更新の際に、暗号化予備鍵記憶手段の暗号化予備鍵を復号鍵で復号した結果を新規復号鍵として復号鍵記憶手段に転送する構成としたので、鍵を暗号化した状態で保存でき、配送鍵の管理（秘匿）を行なう手段を別途設ける必要が無くなる。

【０１１２】なお、第１および第２の実施の形態では、送信局で送信し、受信局で受信する動作を説明したが、受信局の復号鍵を使って暗号化し、送信局の暗号鍵を使って復号化することもできる。

【０１１３】

【発明の効果】以上のように、本発明によれば、暗号通信装置を、鍵配送ごとに更新される予備鍵を用意し、この予備鍵を用いて、制御手段は配送用の鍵が常に暗号通信に未使用の暗号鍵になるように転送順序を制御する構成としたので、未使用の鍵で配送する分だけ安全性が高くなるという効果が得られる。

【０１１４】また、本発明では、一つの鍵を鍵配送と暗号通信に一定の安全性で使用できるので、別に配送鍵の管理（生成・更新）を行なう必要が無くなるという効果が得られる。

【０１１５】また、本発明では、鍵を暗号化した状態で保存できるので、別に配送鍵の管理（秘匿）を行なう必要が無くなるという効果が得られる。

【０１１６】また、本発明では、送信または受信回数をタイミングとして計数手段により計数し、判断手段が一定回数に達したことを通知することにより、定期的に鍵更新を行なう構成としたので、処理が軽くなるとともに、自動で鍵更新が行なわれて、ユーザーに負担がかからなくなるという効果が得られる。

【０１１７】また、本発明では、判断手段により更新情報に依存して鍵の更新のたびにタイミシグを更新するので、情報が盗聴者に知られる可能性が低くなるという効果が得られる。

【図面の簡単な説明】

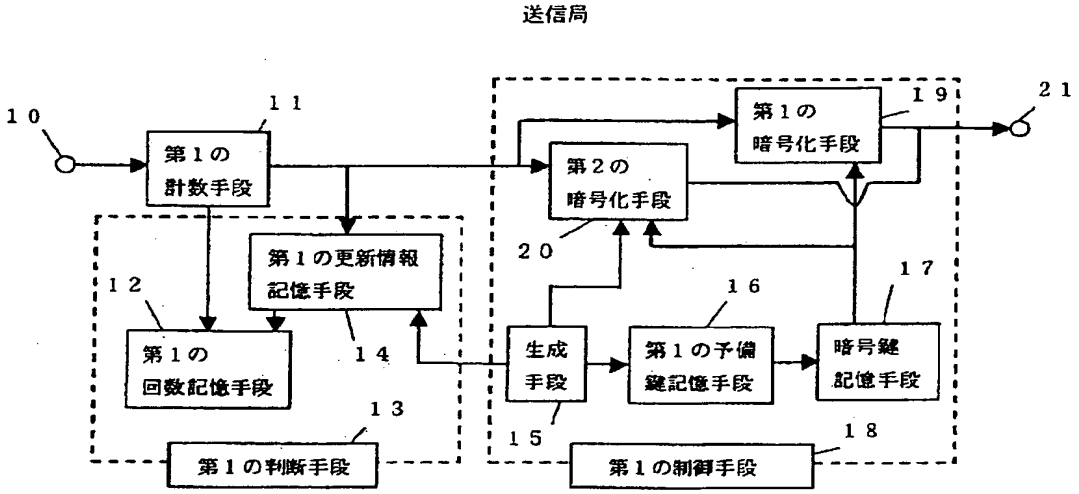
【図１】本発明の第１の実施の形態における送信局の構成を示すブロック図、

【図２】本発明の第１の実施の形態における受信局の構成を示すブロック図、

【図３】本発明の第１の実施の形態における送信局の鍵更新の動作フロー図、

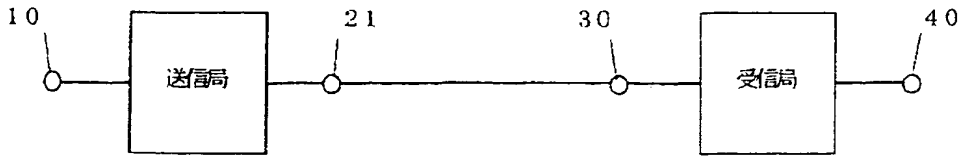
【図４】本発明の第１の実施の形態における受信局の鍵更新の動作フロー図、
【図５】本発明の第１の実施の形態における暗号通信装置の構成を示すブロック図、
【図６】本発明の第１の実施の形態における送信局における鍵の状態のタイミング図、
【図７】本発明の第１の実施の形態における受信局における鍵の状態のタイミング図、
【図８】本発明の第２の実施の形態における受信局の構成を示すブロック図、
【図９】本発明の第２の実施の形態における受信局の鍵更新の動作フロー図、
【図１０】本発明の第２の実施の形態における受信局における鍵の状態のタイミング図、
【図１１】従来の暗号通信装置における送信局の構成を示すブロック図、
【図１２】従来の暗号通信装置における受信局の構成を示すブロック図である。
【符号の説明】
11　第１の計数手段
12　第１の回数記憶手段
13　第１の判断手段
14　第１の更新情報記憶手段
15　生成手段
16　第１の予備鍵記憶手段
17　暗号鍵記憶手段
18　第１の制御手段
19　第１の暗号化手段
20　第２の暗号化手段
31　第２の計数手段
32　第２の回数記憶手段
33　第２の判断手段
34　第２の更新情報記憶手段
35　第２の予備鍵記憶手段
35'　暗号化予備鍵記憶手段
36　復号鍵記憶手段
37　第２の制御手段
38　第１の復号化手段
39　第２の復号化手段

【図１】



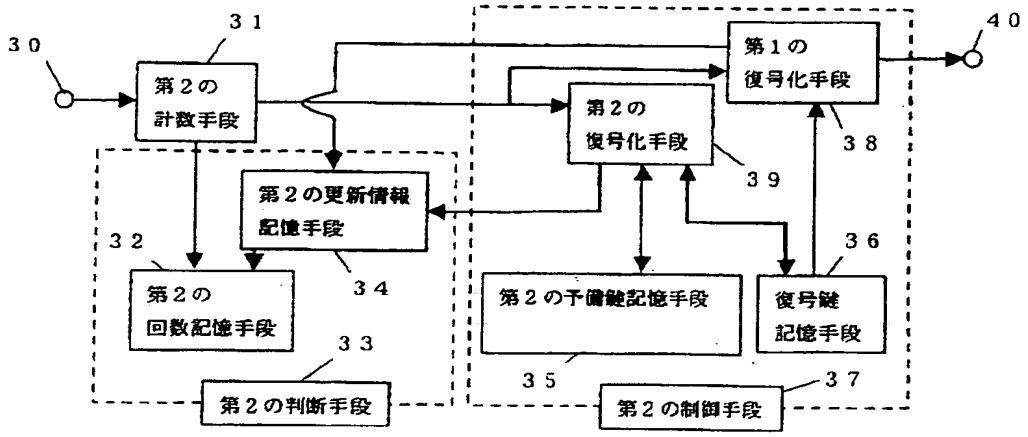
【図５】

暗号通信装置全体



【図２】

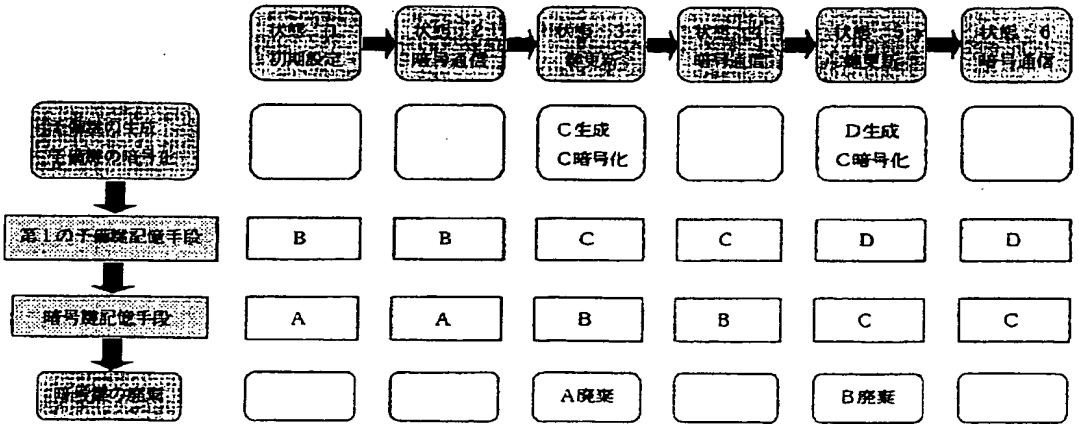
受信局



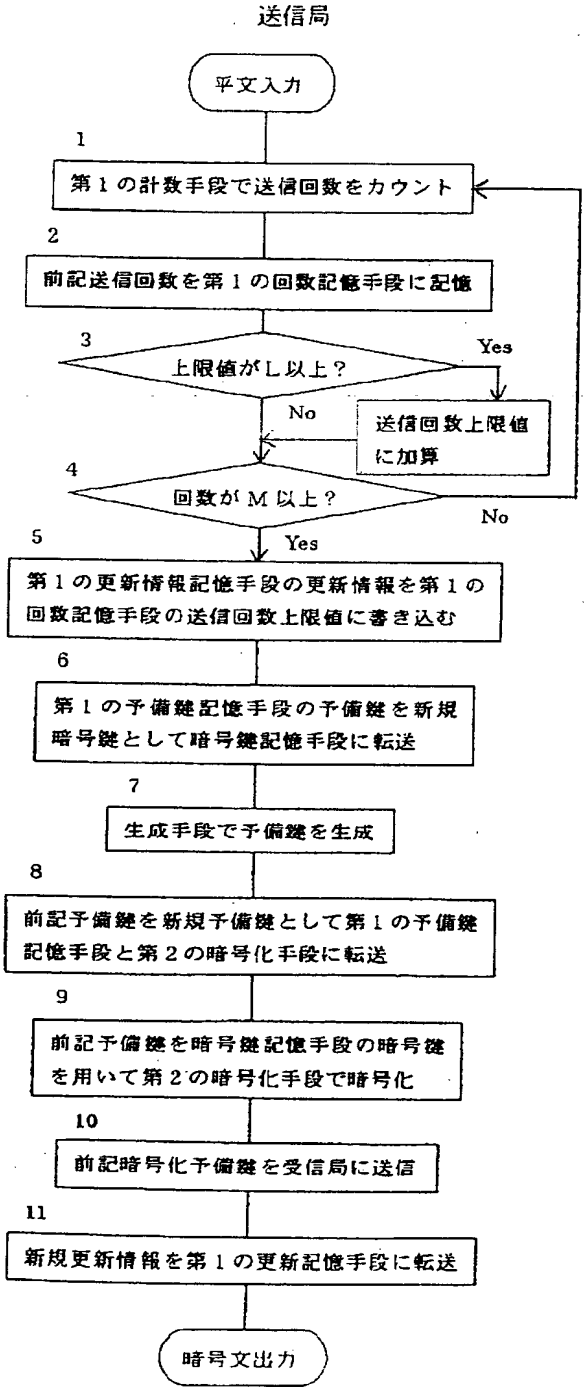
【図６】

鍵の状態

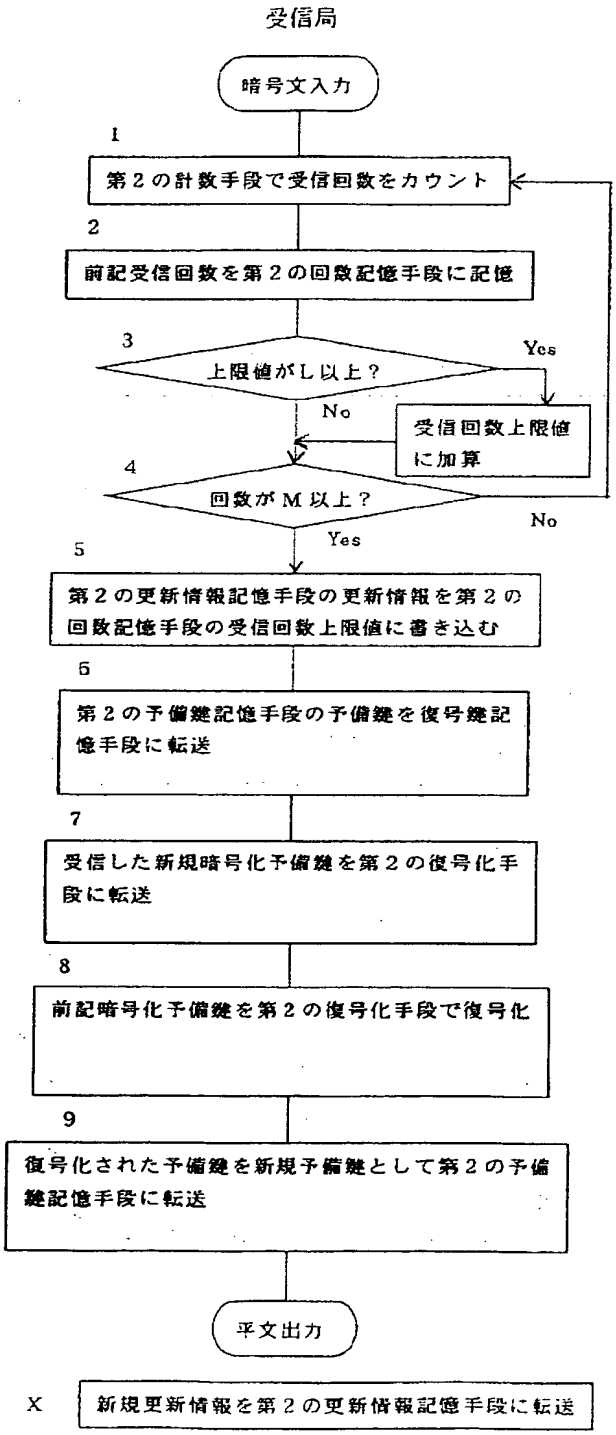
送信局



【図３】



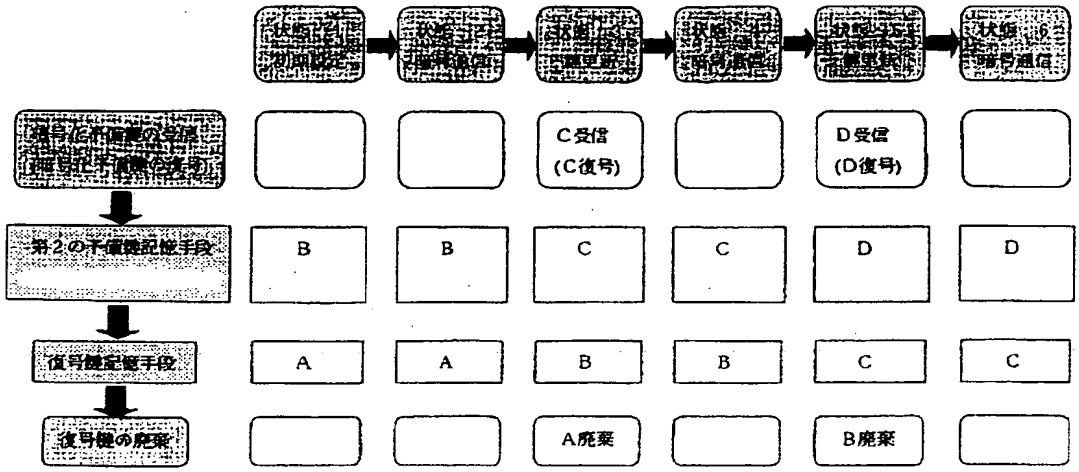
【図４】



※２　Xは更新情報の種類によりタイミングが異なる。

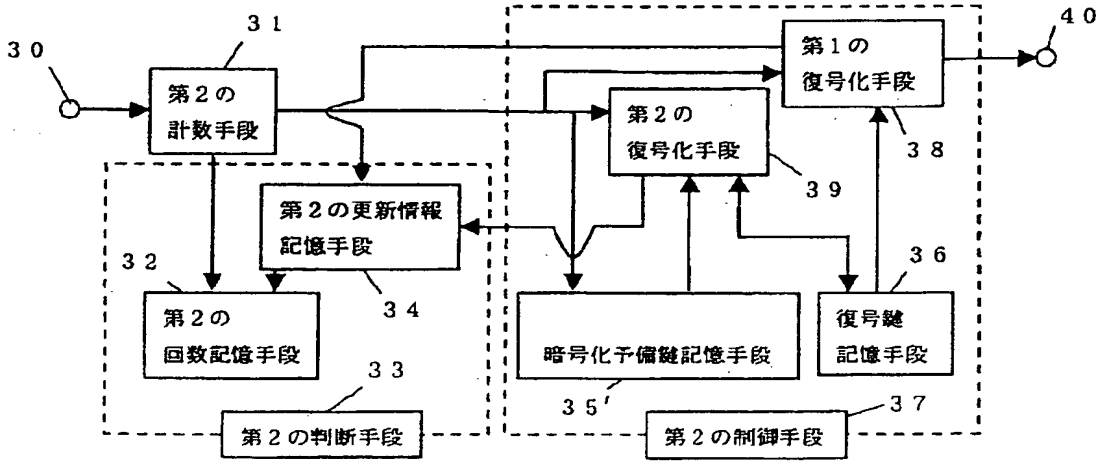
【図７】

受信局

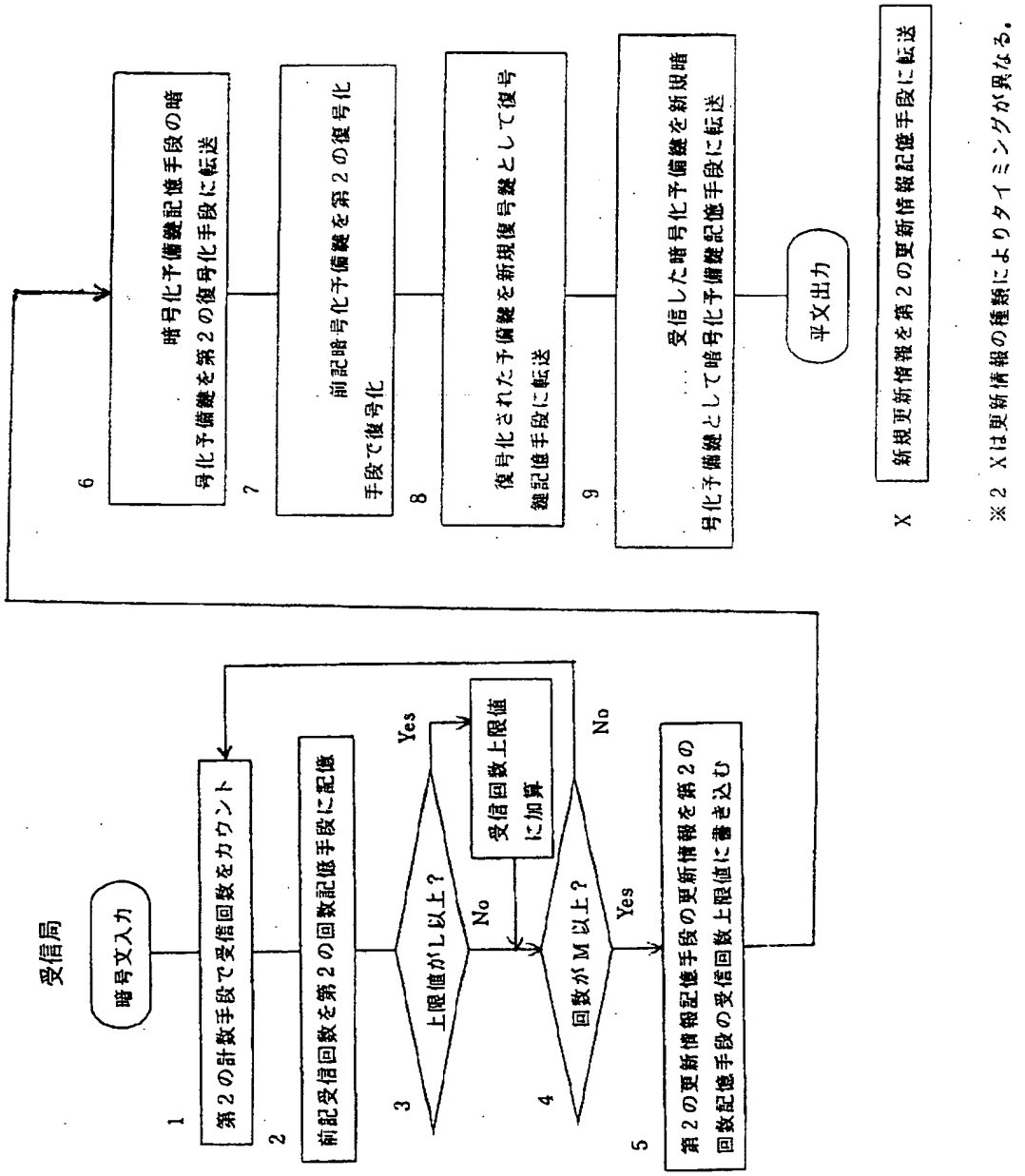

C受信
(C復号)
D受信
(D復号)
第２の予備鍵記憶手段
B
B
C
C
D
D
復号鍵記憶手段
A
A
B
B
C
C
復号鍵の廃棄
A廃棄
B廃棄

【図８】

受信局


３０
３１
第２の
計数手段
第１の
復号化手段
４０
第２の
復号化手段
３８
３９
第２の更新情報
記憶手段
３２
３６
第２の
回数記憶手段
３４
暗号化予備鍵記憶手段
復号鍵
記憶手段
３３
３５
３７
第２の判断手段
第２の制御手段

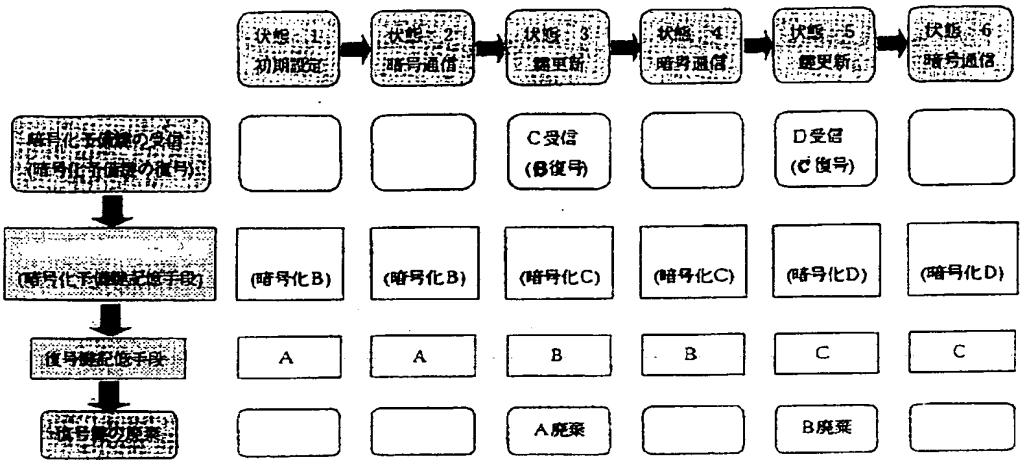
【図９】



※２　Xは更新情報の種類によりタイミングが異なる。

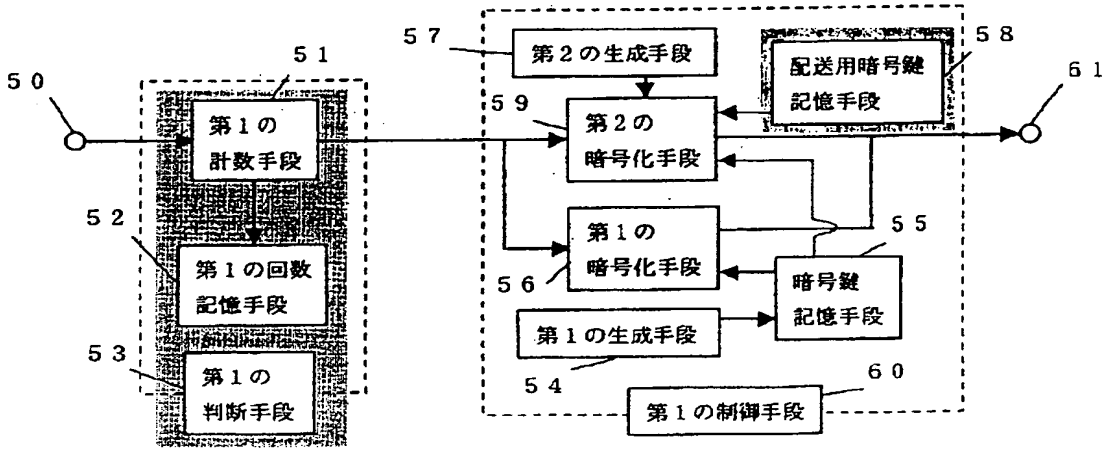
【図１０】

受信局



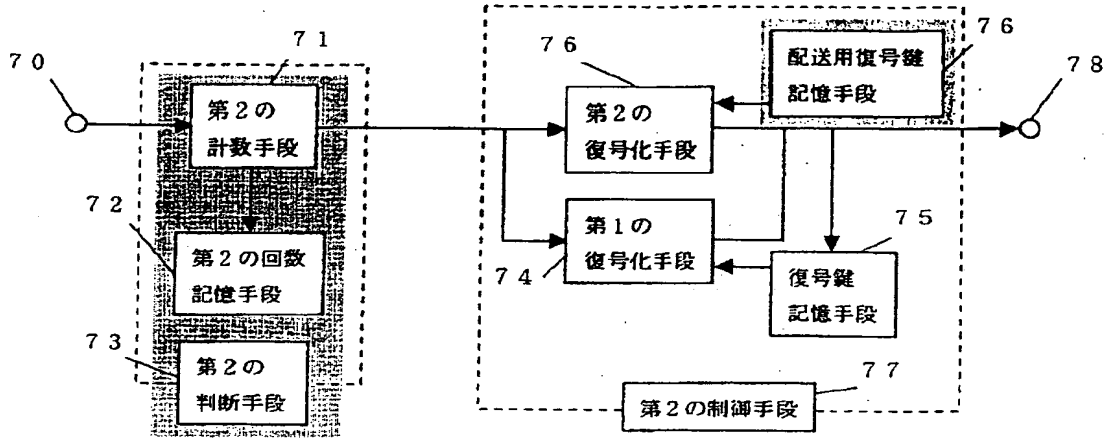
【図１１】

送信局



【図１２】

受信局


７０
７１
第２の
計数手段
７２
第２の回数
記憶手段
７３
第２の
判断手段
７６
第２の
復号化手段
７４
第１の
復号化手段
７６
配送用復号鍵
記憶手段
７５
復号鍵
記憶手段
７７
第２の制御手段
７８